Amendments to the Specification

For the paragraph on page 2, beginning on line 11:

The Internet and the World Wide Web are rapidly expanding, with the number of new devices being connected at a phenomenal rate. A direct result of this expansion is a shortage of Internet Protocol (IP) addresses. Internet Protocol is the fundamental protocol used to route traffic across the Internet. It is typical to assign a globally unique address to each host attached to the Internet that use TCP/IP. However, in order to extend the life of the current IP addressing scheme (i.e., IPv4), address registries are requiring more justification before an organization can acquire additional IP addresses. Thus, an organization may not have enough assigned globally unique IP addresses to ~~dedicated~~ dedicate one to each host computer desiring global connectivity.

For the paragraph on page 3, beginning on line 1:

For example, private enterprise networks can number their hosts according to the methodology proposed in "Address Allocation for Private Internets", RFC 1918. A NAT router is placed at the border of the private enterprise network and is used as an interface to the Internet or other external network. The NAT router allows a host within a private enterprise to communicate with another host on the Internet (i.e., outside the private enterprise network) by translating the IP address of the private enterprise host to and from a globally unique IP address. To allow a host within the private network to be accessed by a host external to the private network, the NAT address translation must be known prior ~~a priori~~, and be statically defined. The NAT router can then use this static address translation to translate the predetermined globally unique IP address to the private network address of the host. This NAT approach works well when the number of hosts desiring global connectivity is equal to or less than the number of globally unique IP numbers assigned to the NAT router. Network address translation and its use is further described in "The IP Network Address Translator (NAT)", RFC 1631.

For the paragraph on page 4, beginning on line 8:

According to the invention, a method and apparatus are disclosed for dynamically assigning a public network address for a private network host in response to a request generated external to the private network. A requesting host desiring access to a host within the private network queries a domain name server for the public network address of the private network host. Then, the domain name ~~sever~~ server queries a network address translator for the private network, and receives a reply indicating a dynamically allocated public network address for the specified private network host. The requesting host can then use this returned public network address for communicating with the private network host. In this manner, a set of public addresses can be shared, with a public network address being dynamically allocated to a private network host in response to a request for access by a host external to the private network.

For the paragraph on page 5, beginning on line 21:

An embodiment of a method of the present invention provides for operating a computer system to respond to a domain name service query for a public address of a private network host. This method preferably comprises the steps of: receiving the domain name service query from a requesting host for the ~~pubic~~ public address of the private network host; sending a request to a network address translator for the ~~pubic~~ public address of the private network host; receiving a reply from the network address translator containing the ~~pubic~~ public address of the private network host; and sending the ~~pubic~~ public address of the private network host to the requesting host. Preferably, the public address is an Internet Protocol (IP) address. Preferably, the request to the network address translator is in a Simple Network Management Protocol format.

For the paragraph on page 6, beginning on line 3:

Preferably, the method further comprises the step of updating an address data structure in response to receiving the ~~pubic~~ public address of the private network host. Preferably, the reply from the network address translator includes a time period in which the ~~pubic~~ public address of the private network host is valid; and the method further comprises the step of updating the address data structure in response to the public address of the private network host not being valid. Preferably, the time period specifies a time duration of network inactivity for the public address. Preferably, the method further comprises the steps of: receiving a time-out message from the network address translator for the ~~pubic~~ public address of the private network host; and updating the address data structure in response to receiving the time-out message.

For the paragraph on page 9, beginning on line 9:

For illustration purposes, certain ~~element~~ elements of FIG. 1 have a domain name and/or an IP address. In this exemplary configuration, requesting public host 139 has domain name "public_host.public.net" with IP address 198.6.250.9; public network interface 125 of network address translator 100 has IP address 144.230.1.2; private network interface of network address translator 100 has IP address 10.0.1.1; network interface 175 of domain name server 150 has domain name "dns.private.net", a private network IP address of 10.0.1.5, and a public IP address of 144.230.1.5; private network host 197 has domain name "host_a.private.net" and IP address of 10.0.1.7; and private network host 198 has domain name "host_b.private.net" and IP address of 10.0.1.8. The public IP address for network interface 175 of domain name server 150 is permanently defined in an address data structure of network address translator 100 to allow domain name server 150 to receive DNS requests from hosts outside private network 140. As would be understood by one skilled in the art, the exemplary domain names and IP addresses presented and discussed with reference to FIGS. 1-5 are used to help better describe the present invention, with the present invention not being so limited to this illustrated configuration.

For the paragraph on page 11, beginning on line 19:

Next, if domain name server 150 receives an DNS query as determined in step 330, then if the DNS query is for a host having a valid address in the address data structure as determined in step 340, then the address is retrieved from the address data structure and sent to the requesting host in step 345. This address could either be a valid public address for a private network host or a valid private network address depending on the request host. Otherwise, if the request ~~if~~ is for a public address for a known private address as determined in step 350, then a request is sent in step 360 to the network address translator 100 for the public address of the private network host specified in the original DNS query. If a responsive message is received as determined in step 370, domain name server 150, in step 380, relays the public address of the private network host to the request host. Otherwise, a message is sent to the requesting host that the address is unknown for the host specified in the DNS query (steps 355, 375). Processing then returns to the top of the loop (step 310) to repeat the processing of steps illustrated in FIG. 3.